Stockholms stad

Ledningens genomgång år 2025 samt 3-årsplan

S:t Erik Markutveckling

Beslutad 2025-10-xx
Reviderad [datum]

Ledningens genomgång

Dnr: STEM 2025/286

Kontaktperson: Johan Gagner

Ledningens genomgång är ett begrepp inom informationssäkerhet som syftar till att de som ansvarar för informationssäkerheten inom en organisation, minst årligen ska informera sig om hur arbetet går.

Enligt Stockholms stads tillämpningsanvisning för informationssäkerhet ska förvaltningschef/bolagschef inhämta en rapport, så kallad ”Ledningens genomgång” från informationssäkerhetssamordnaren. Rapporten bör exempelvis redogöra för om det finns lokala rutiner för incidenthantering, för utbildning av medarbetare och om informationsklassningar och registerförteckning är genomförda.

Denna rapportering ska ge information och underlag till förvaltningschef/bolagschef att årligen bedöma om det lokala informationssäkerhetsarbetet och dataskyddsarbetet är tillräckligt och har önskad verkan. Förvaltnings- och bolagschefer ska ta upp aktiviteter som rör informationssäkerhet och dataskydd i verksamhetsplaneringen och i det interna arbetet med att uppnå tillräcklig intern kontroll.[1]

I *Anvisningar för nämndernas arbete med verksamhetsplan 2024* uppmanades samtliga nämnder och bolagsstyrelser att ta fram en Ledningens genomgång med en planering för informationssäkerhetsarbetet under de efterföljande tre åren. Denna bilades verksamhetsplanen. *Riktlinje för informationssäkerhet* i Stockholms stad följdes i denna planering.

Dessa aktiviteter redovisas i Ledningens genomgång. Inventering och informationsklassning är grunden i informationssäkerhetsarbetet.

Alla nämnder och bolagsstyrelser ska prioritera att ta fram en plan för att inventera och klassa information som används i verksamheten alternativt se över och uppdatera genomförda klassningar.

[1] Tillämpningsanvisning till stadens riktlinje för informationssäkerhet

Innehållsförteckning

1 Ledningssystem för informationssäkerhet, LIS

Stockholms stads arbete med informationssäkerhet utgår från en så kallad ISO standard, ISO 27001. Det är en global standard för informationssäkerhet som hjälper organisationer att skydda sin känsliga information från hot och risker. Standarden ger ett ramverk för hur man implementerar ett ledningssystem för informationssäkerhet, LIS, som skyddar informationstillgångarna och ger en IT-process som är lättare att hantera, mäta och förbättra.

Stockholms stads informationssäkerhetsarbete regleras i en tillämpningsanvisning som är en bilaga till stadens Kvalitetsprogram[2]. Till riktlinjen finns tillämpningsanvisningar som är fastställda av stadsdirektören.

Tillämpningsanvisningarna reglerar ansvar och roller sett till Stockholms stads systematiska informationssäkerhetsarbete. För S:t Erik Markutvecklings räkning har VD fastställt en så kallad lokal anvisning som beskriver hur stadens övergripande ledningssystem för informationssäkerhet omhändertas inom bolaget.

1.1 Vad påverkar S:t Erik Markutvecklings informationssäkerhetsarbete?

För att upprätthålla ett informationssäkerhetsarbete som är aktuellt över tid ska S:t Erik Markutveckling ha ett riskbaserat förhållningssätt i sitt informationssäkerhetsarbete. Det innebär att verksamheten ska arbeta med att identifiera, bedöma och följa upp de informationssäkerhetsrisker som kan uppstå i verksamhetens informationshantering.

1.1.1 Omvärldsbevakning (Om bolagets verksamhet med avseende på dataskydd och informationsteknik)

S:t Erik Markutveckling äger, förvaltar och utvecklar fastigheter i Stockholm i avvaktan på att de ska omvandlas till bostäder, arbetsplatser eller trafikplatser. Bolagets verksamhet inriktar sig på förvärv, förvaltning, uthyrning och utveckling till så god avkastning som möjligt med hänsyn tagen till stadens utveckling.

Bolaget hanterar för egen del en begränsad del känslig information i digitala system då en stor och viktig del av bolagets

[2] Stockholms stads kvalitetsprogram (start.stockholm)

informationssäkerhetsarbete hanteras av extern fastighetsförvaltning. Fastighetsförvaltande organisation hantera till exempel fastighetsdokumentation och hyresgästuppgifter, vilket regleras i avtal mellan förvaltande bolag och S:t Erik Markutveckling. S:t Erik Markutveckling ska dock säkerställa att alla känslig information som behandlas kopplat bolagets uppdrag hanteras på ett ändamålsenligt och säkert sätt.

1.1.2 Bolagets organisation avseende riskhantering

S:t Erik Markutveckling organisation för informationssäkerhet är indelad i tre olika nivåer. Den **styrande** omfattar operativt beslutande roller och funktioner i verksamheten. Dessa har på olika nivåer en budget och ett personalansvar, vilket även innefattar operativt ansvar för informationshanteringen inom den delen av verksamheten.

De **stödjande** och **granskande** funktionerna är specialistfunktioner som stödjer linjeverksamheten i dess informationssäkerhetsarbete. De granskande funktionerna, utöver stadens egna revisorer, följer även upp att riktlinjer och lagstiftning följs.

Stadens arbete med risk- och sårbarhetsanalys (RSA) bedrivs i en tvåårscykel. En ny cykel inleddes under 2024. Vad avser RSA hanteras dessa risker av verksamheten i samarbete med bolagets ovan beskrivna riskhanteringsfunktion. Varje risk har en riskägare och åtgärdsplan (såvida inte risken accepteras). Riskhanteringsfunktionen rapporterar risknivåer, riskhantering m.m. till styrelsen vid behov. Riskhanteringsfunktionens arbete kontrolleras av internrevisionen.

1.1.3 Risker som identifierats i GDPR-årsrapport

Dataskyddsombudet har i årsrapporten för 2024 skrivit att:

- Central objektförvaltning har inte tillräckligt med resurs och kan inte svara mot lokal (STEM:s) objektförvaltning. (Ny)
- Ny teknik, t.ex. behandling av personuppgifter och annan information behandlas med AI utan korrekt analys och dokumentation. (Ny)
- Tredjelandsöverföringar (Kvarstår)
- Osäker e-posthantering med personuppgifter (Kvarstår)

- **Granskning, Personuppgiftsbiträde.**
  I årsrapporten för 2023 skrev jag som dataskyddsombud: *”Bristen som kvarstår att granska till 2024 är att kommunikationsvägarna för registrerade d.v.s. den*

allmänna e-postadressen omhändertar frågor om dataskydd och eventuella begäran från registrerade fungerar.”

Under 2024 upphandlades förvaltarrollen och denna granskning blev istället för att kontrollera kommunikationsvägar, följa upp befintliga avtal för att eventuellt avsluta tjänsten. Detta perspektiv omhändertogs tillsammans med informationssäkerhetssamordnaren och dataskyddshandläggaren.

2 Förbättringar för verksamhetens LIS

2.1 S:t Erik Markutvecklings lokala anvisning för informationssäkerhet

Den 15 september 2023 fastställde Vd bolagets Lokala anvisning för informationssäkerhet.
Anvisningen är diarieförd och finns tillgänglig för alla medarbetare på bolagets gruppdisk.

I samband med verksamhetsberättelse och bokslut tar bolaget del av dataskyddsombudets årsrapport och stor hänsyn tas till eventuella rekommendationer till personuppgiftsansvarig som lämnas i rapporten.

3 Åtgärder 2025

Under året har bl a nedan arbete utförts:

- informationsklassningar
- uppdaterat organisation enligt PM3 (light)
- översyn av hanteringsrutin för informationssäkerhetsincidenter
- översyn av lokal anvisning för informationssäkerhet
- medarbetare har genomfört Stadens utbildningar i informationssäkerhet och dataskydd

4 Åtgärder 3-årsplan

4.1 Under 2026 ska S:t Erik Markutveckling

- årligen genomföra och dokumentera informationsklassningar
- påbörja arbete med att åtgärda de risker framtagna i riskanalys 2024, se dokument ”STEM_Riskanalys 2024.xlsx”, Länk
- uppdatera kontinuitetsplaner/avbrottsplaner.
- säkerställa att informationssäkerhetsfrågorna lyfts fram och ingår i det interna utvecklingsarbetet
- se till att samtliga medarbetare genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
- uppföljningar av registret över personuppgiftsbehandlingar utförs.
- årlig översyn av Lokal anvisning för informationssäkerhet
- årlig uppdatering av Lokal incidenthanteringsrutin
- etablera en rutin för regelbundna behörighetsrevisioner (identitet och åtkomst)
- uppföljningar av övrig rutindokumentation utförs

4.2 Under 2027 ska S:t Erik Markutveckling

- årligen genomföra och dokumentera informationsklassningar
- se till att samtliga medarbetare genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
- uppföljningar av registret över personuppgiftsbehandlingar utförs.
- årlig översyn av Lokal anvisning för informationssäkerhet
- årlig uppdatering av Lokal incidenthanteringsrutin
- årlig behörighetsrevision (identitet och åtkomst)
- uppföljningar av övrig rutindokumentation t ex avbrottsplan och behörighetsrevision utförs
- öva utifrån kontinuitetsplaner/avbrottsplaner.

4.3 Under 2028 ska S:t Erik Markutveckling

- årligen genomföra och dokumentera informationsklassningar
- se till att samtliga medarbetare genomför stadens obligatoriska e-utbildningar för informationssäkerhet och dataskydd
- uppföljningar av registret över personuppgiftsbehandlingar utförs.
- årlig översyn av Lokal anvisning för informationssäkerhet
- årlig uppdatering av Lokal incidenthanteringsrutin
- årlig behörighetsrevision (identitet och åtkomst)
- uppföljningar av övrig rutindokumentation t ex avbrottsplan och behörighetsrevision utförs.
- öva utifrån kontinuitetsplaner/avbrottsplaner.